

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Andrew Nagy
Julio Ordonez
Tharsini Yogaratnam
Alexandra Wong
Brensley Edmondson
Kamran Maroussi

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



Normal Activity

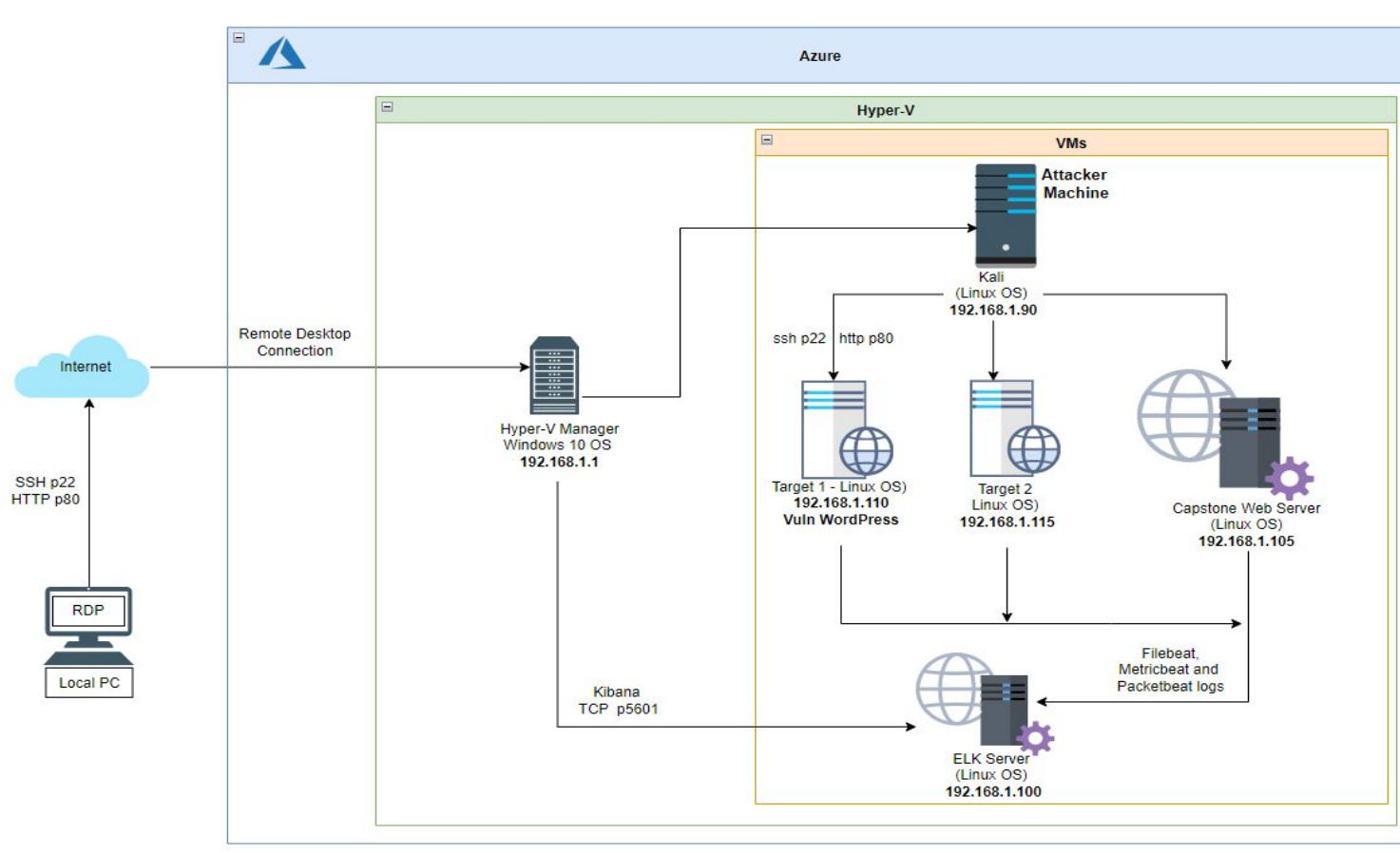


Malicious Activity



Network Topology & Critical Vulnerabilities

Network Topology



Network

Address Range:
192.168.1.0/24
Netmask:255.255.255.0
Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Lack of perimeter protection against malware.	Perimeter protection would scan all inbound files for malware and viruses.	User was able to download malware from Internet.
Lack of endpoint protection against malware.	Endpoint protection would scan all inbound files for malware and viruses.	User was able to download and save malware from Internet.
Lack of perimeter white listing of Internet sites.	Perimeter protection would allow access to white listed websites and IP addresses.	User was able to visit IP address that is black listed according to https://www.ipvoid.com
Lack of protection against content outside of organization's acceptable use policy.	BitTorrent does not normally have a business requirement.	User was able to download torrent file.
Lack of password policy for Wordpress.	There appears to be no minimum requirements for password complexity, account timeouts etc.	A bad actor can brute force the admin login.
Poorly configured Wordpress Instance.	Lack of restrictions around file permissions, connecting to MySQL with Root.	Provides access to the SQL account credentials set within the wp_config.php file. Root account has full control of the database.
Sudo privileges to python	The user Steven has sudo access to python.	A bad actor can escalate privileges to root via python.

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
phpMailer 5.2.17	Old version of software subject to CVE: 2016-10033. (https://packetstormsecurity.com/files/140280/PHPMailer-5.2.17-Remote-Code-Execution.html)	Able to launch a remote shell as web site user 'www-data'.
Default content files left in place.	Some files contain configuration information.	Exposure of information to make reconnaissance easier.

The background of the slide is a dark gray field filled with a complex, repeating pattern of geometric shapes. These shapes include various sizes of triangles and squares, some of which are slightly lighter or darker than the background, creating a subtle, textured effect. The overall aesthetic is modern and minimalist.

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	1) 172.16.4.205 2) 10.0.0.201 3) 185.243.115.84	Machines that sent the most traffic.
Most Common Protocols	1) TCP(85.7%) 2) UDP(14.1%) 3) OTHER(0.02%)	Three most common protocols on the network.
# of Unique IP Addresses	1) 811	Count of observed IP addresses.
Subnets	1) 10.6.12.0/24 2) 172.16.4.0/24 3) 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	1) june11.dll	Number of malware (trojan) binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

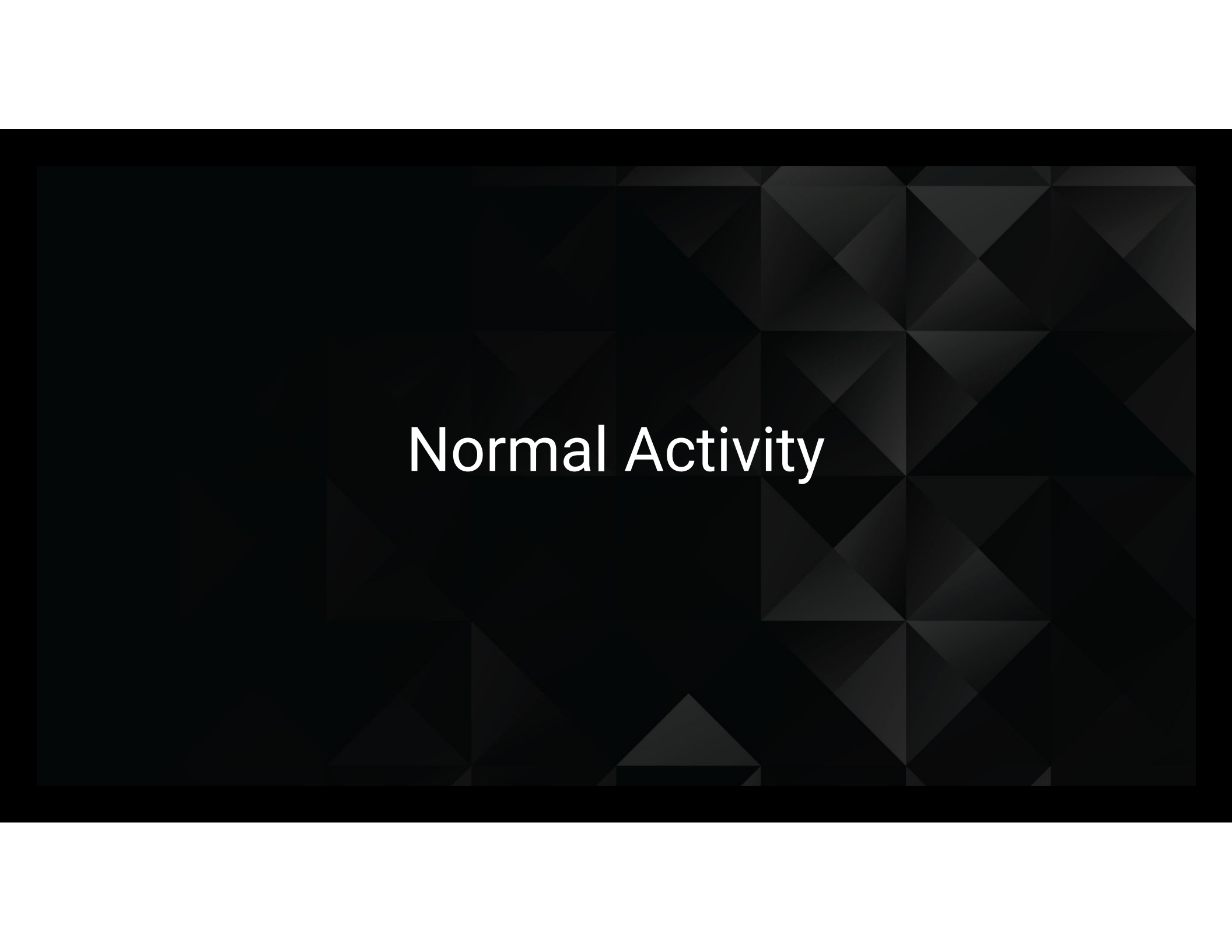
- Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Watching Youtube videos
- Looking into medical services
- Training Module/Trivia Game
- Looking into Bicycle Events and Cycling Tips

Suspicious Activity

- Downloading Copyrighted Materials
- AD Server and Downloaded Malware
- Infected Windows Machine



Normal Activity

Summarize the following:

- The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main window is divided into three panes: the packet list pane on the left, the packet details pane in the middle, and the packet bytes pane on the right. The packet list pane shows a list of captured packets, with the first packet selected. The packet details pane shows the hierarchical structure of the selected packet, with the 'dns contains youtube' entry highlighted. The packet bytes pane shows the raw data of the packet.

```

.....[.....
}]?81
ncv..P4(.....G.ob..+./.$.#.(.
.....=<5./
.....fomatch.youtube.com.....
.....#.....h2.http/1.1.....
.....H...D...[j...Y..8XG.o*?y.v(\j2.0.eJ.....
+.....h2.....0...0..w.....S..r...0
*..H..
.....0T1.0...U...US1.0..U.
..Google Trust Services1%0..U....Google Internet Authority G30..
180619114216Z.
18082813209Z0f1.0...U....US1.0..U..
California1.0...U..
Mountain View1.0...U.

Google LLC1.0...U...google.com@Y0...*.H.=...*.H.=...B...EW...>.....
7.Y...DB.E...f..z..eF.U.../HZ.....&...z.....0...U.%..0
+.....0...U.....0...U...0.....*google.com.
.android.com.*.appengine.google.com.*.cloud.google.com.*.db833953.google.cn.*.g.co.*.gcp.gvt2.
com.*google
analytics.com.*google.ca.*google.cl.*.google.co.in.*.google.co.jp.*.google.co.uk.*.google.co
m.ar.*.google.com.au.*.google.com.br.*.google.com.co.*.google.com.mx.*.google.com.tr.*.google
.com.vn.*.google.de.*.google.es.*.google.fr.*.google.hu.*.google.it.*.google.nl.*.google.pl.*
.google.pt.*.googleapis.com.*.googleapis.com.*.googlecommerce.com.*.googlevideo.com.*.gstatic.
cn.*gstatic.com.
*.gvt1.com.
*.gvt2.com.*.metric.gstatic.com.*.urchin.com.*.url.google.com.*.youtube-nocookie.com.
*.youtube.com.*.youtubeeducation.com.*.yt.be.*.yting.com.android.clients.google.com.android.com.
developer.android.google.cn.developers.android.google.cn.g.co.goo.gl.google-analytics.com.
google.com.googlecommerce.com.source.android.google.cn
urchin.com.
www.goo.gl.youtu.be.youtube.com.youtubeeducation.com.yt.be0h.....0z0+.....0!http://
pki.goo.gsrz/GTSGIAG3.crt0)+.....0..http://ocsp.pki.goog/GTSGIAG30.....\!+V10..Gc.P.Y.H.
0...U...0.0..U.#.0..W.P.gvv.....K01.U...0.0.
+.....y..0...0.....01.U...0(08$.*http://crl.pki.goog/GTSGIAG3.crt0
*..H..
.....a.....a.[.G..LQ...uS.vPz.....U6rV@lg.....U.U.C.20..c
N..F...A.YSz.....R.
QZ.....
a.$.....R.E...w9I...uJ.V.VK...>W[X..SE*!<.....N..k.T.T.T.*p..h.....i'.J>.....
[.....hb.Ky.\S.K.s.\J.F.\X.....[.....c0Z.....5.v3.....SIC.....0..0..D...
+.....r.8Z.S0..
*..H..
.....0L1.0...U...GlobalSign Root CA - R21.0..U.

```

4 client pkts, 6 server pkts, 5 tumors.

Normal #2: Looking into medical services

The screenshot displays a Kali Linux desktop environment. In the background, a web browser is open to the website <https://www.sabethahospital.com>. The website header includes the address "14th & Oregon Street | Sabetha," and a navigation menu with links: Home, About Us, Hospital, Family Practice, Home Health & Hospice, Monthly Health Topics, Services, Visitor Information, and SCH Volunteer. A prominent banner for "Capture Rx Security Incident" features a red padlock icon surrounded by a green circular graphic.

In the foreground, the Wireshark network traffic analysis tool is open, displaying a packet capture file named "WireShark.pcapng". The main packet list shows several HTTP GET requests from the local machine (DESKTOP-B49J3FD) to the Sabetha Hospital website. The selected packet (16:12:07.636077400) is an HTTP GET request for the file `/common_js/font-awesome-4.7.0/css/font-awesome.min.css`. A detailed view of this packet is shown in the lower pane, displaying the raw HTTP request and response data.

The detailed view of the selected packet (16:12:07.636077400) shows the following information:

GET /common_js/font-awesome-4.7.0/css/font-awesome.min.css HTTP/1.1
Referer: http://www.sabethahospital.com/getpage.php?name=whatappendixdo
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362
Host: www.sabethahospital.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 11 Nov 2019 22:22:20 GMT
Server: Apache
Last-Modified: Tue, 17 Nov 2015 17:15:46 GMT
ETag: "1268291-3029-524bfad283480"
Accept-Ranges: bytes

The bottom pane of Wireshark shows the DNS traffic, including a standard query for `0xfd32 A www.sabethahospital.com` and a standard query response from `12.133.50.21`.

Normal #3: Training Module/Trivia Game

Summarize the following:

- Protocols used for this behaviour include TCP and HTTP, as seen in the screenshot below (initial filter used “tcp contains google”):

The screenshot displays a Wireshark network traffic analysis. The top pane shows a list of network packets. The selected packet (No. 35310) is a TCP segment from a local source to s3-website-us-west-2.amazonaws.com. The bottom pane shows the details of this TCP stream, including the HTTP request and the embedded JavaScript code.

No.	Time	Source	Destination	Protocol	Length	Info
35029	475.423516300	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP	74	56447 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=
35107	476.064810800	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP	60	56447 → 80 [ACK] Seq=1 Ack=1 Win=14720 Len=0
35108	476.073744900	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	HTTP		
35300	478.219936100	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35302	478.243489100	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35304	478.267006700	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35306	478.290563400	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35307	478.291498200	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35310	478.337623800	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35311	478.338569500	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35313	478.362134700	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35314	478.363069800	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35315	478.364087500	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		
35319	478.744210000	e3d93e943791fa0e24193a0a5dc9de4f. local	s3-website-us-west-2.amazonaws.com	TCP		

Details of the selected packet (No. 35310):

- Frame 35310: 478.337623800: s3-website-us-west-2.amazonaws.com → 192.168.1.100:80 [ACK] Seq=1 Ack=1 Win=14720 Len=0
- Details: X-Amz-Request-Id: F7F9A8B0BAED7300, Date: Mon, 11 Nov 2019 22:21:40 GMT, Last-Modified: Thu, 26 Oct 2017 23:25:09 GMT, ETag: "1fb00c3c32abdd17ae5dc7b092b5b302", Content-Type: application/javascript, Content-Length: 14127, Server: AmazonS3
- JavaScript code snippet:

```
use strict;

/*
 * This is the base course model and will give you the start to loading the course
 * Content via XML, and giving you the example of how to mark the course complete
 * or move to the next course.
 * This will vary with every project and every design, but is a good starter
 */

(function() {
  /** Sets up your course object */
  var GetMore = function() {
    var that = this;

    this.poll = this.pollForContent();
    this.data = null; // xml
    this.SpeedRoundAnswers = [];
    this.actorName = 'Anonymous';
    this.actorEmail = 'anonymous@chromebooktrivia.com';
    this.team = {
      objectType: 'Group',
      name: 'Other',
      account: {
        name: 'Other',

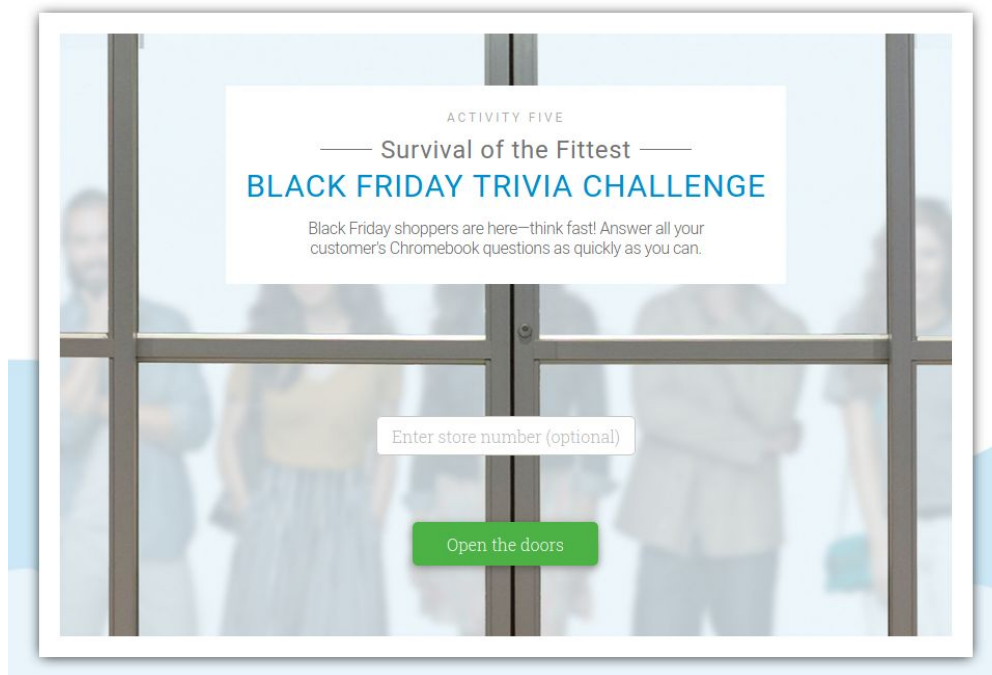
```

Upon following the TCP stream, we noticed the usage of TinCan API, which tracks the interactions of the user with the elements on screen, typical of modern eLearning modules, even though these interactions appeared to be tracked as an anonymous user.

Normal #3 (cont): Training Module/Trivia Game

Summarize the following:

- The user was accessed and interacted with a trivia challenge activity, located at <http://www.chromebooktrivia.com>. From the records, we can see that the server is located in AWS.



Normal #4: Looking into Bicycle Events and Cycling Tips

Summarize the following: Your include HTTP and TCP, as seen in the screenshot below (initial filter used “tcp contains google”):

The image displays two screenshots from the Wireshark network protocol analyzer. The left screenshot shows a list of captured packets filtered by 'tcp.stream eq 520'. The right screenshot shows the detailed view of the selected HTTP 200 OK packet.

No.	Time	Source	Destination	Protocol
53979	637.425744100	10.11.11.121	orbike.com	TCP
53983	637.430346500	10.11.11.121	orbike.com	TCP
53985	637.441169700	10.11.11.121	orbike.com	HTTP
53995	637.610378000	10.11.11.121	orbike.com	TCP
53996	637.611422400	10.11.11.121	orbike.com	TCP
53997	637.612476000	10.11.11.121	orbike.com	TCP
53998	637.613530200	10.11.11.121	orbike.com	TCP
53999	637.614589600	10.11.11.121	orbike.com	TCP
54000	637.615637600	10.11.11.121	orbike.com	TCP
54001	637.616695200	10.11.11.121	orbike.com	TCP
54002	637.617751400	10.11.11.121	orbike.com	TCP
54007	637.630697100	10.11.11.121	orbike.com	HTTP
54018	637.803356900	10.11.11.121	orbike.com	TCP
54019	637.804409200	10.11.11.121	orbike.com	TCP

Wireshark - Follow TCP Stream (tcp.stream eq 520) - part_3.pcapng

GET / HTTP/1.1
Host: orbike.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-N950U AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/10.1 Chrome/71.0.3578.99 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ko-KR;q=0.8,ko;q=0.7
Cookie: _ga=GA1.2.2905005.1573510360; _gid=GA1.2.1395558662.1573510360

HTTP/1.1 200 OK
Server: openresty
Date: Mon, 11 Nov 2019 22:24:23 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Link: <http://orbike.com/wp-json/>; rel="https://api.w.org/"
X-TEC-API-VERSION: v1
X-TEC-API-ROOT: http://orbike.com/wp-json/tribe/events/v1/
X-TEC-API-ORIGIN: http://orbike.com
Content-Encoding: gzip
X-Varnish: HIT
Age: Mon, 11 Nov 2019 22:12:38 GMT

250a
.....XmS....P..\$.I...Z...3...p0(K.Ql...+)...C...=.....gW..v.
9(.....@F!.....C.i.e.]o[I..]-.x.l.....J.b.ZV....@..iY.....M.).{a.....
..4=.i.....q...).3m.....
.8.....N.t.h.o.....3"W,6S\.=.b)..9..%-.;...m...AD\$N!..)@...f.\$.
4...h...M.....!.....p....lyTHN{.u.....W.9.1)rr}.l.#..

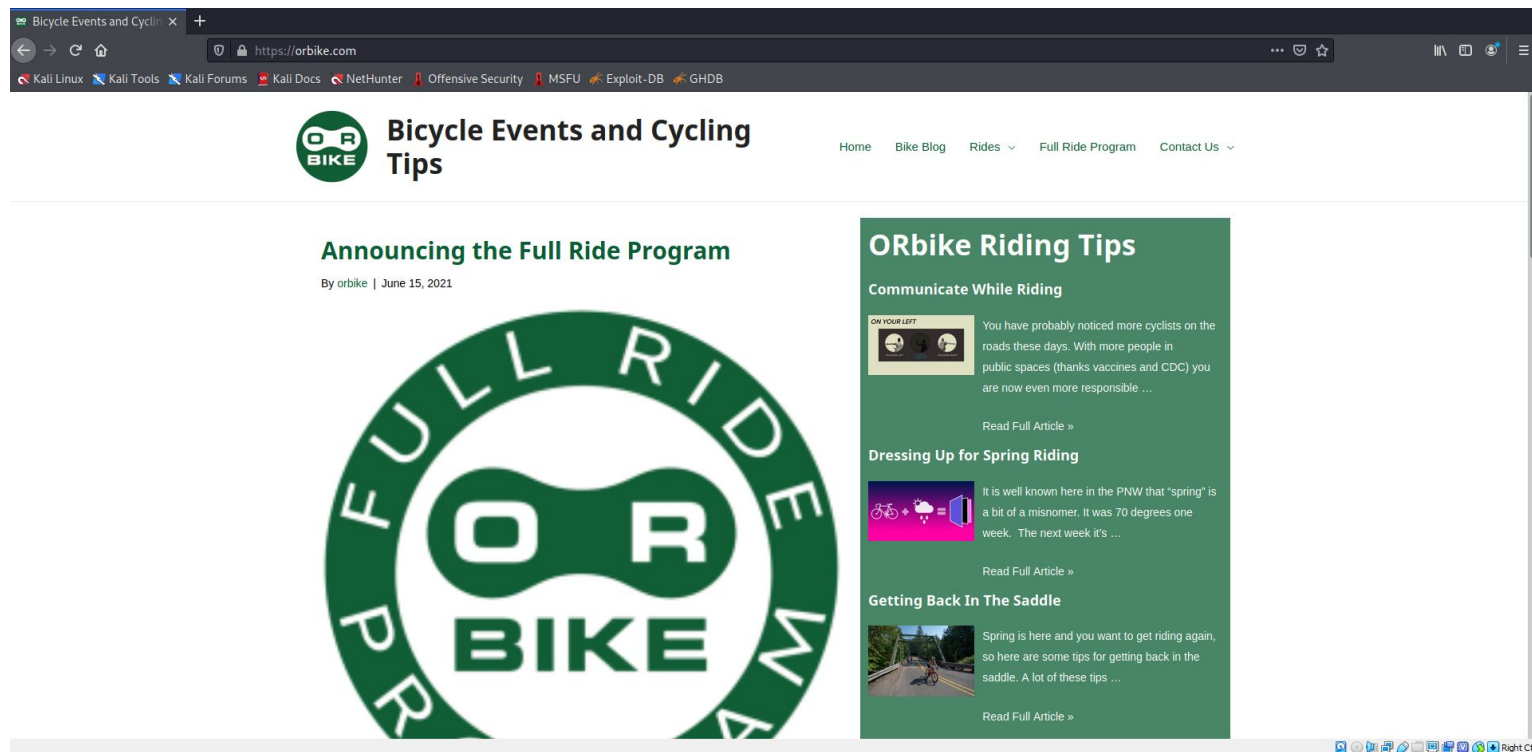
2 client pkts, 16 server pkts, 3 turns.
Entire conversation (20kB) Show data as ASCII Stream 520
Find: Filter Out This Stream Print Save as... Back Close Help

Looking closer at the HTTP request, we can see that the user went to this page via Google as specified in the **Referer** field of the request.

Normal #4 (cont): Looking into Bicycle Events and Cycling Tips

Summarize the following:

- The user was browsing a Bicycle Events and Cycling tips, located at <https://orbike.com>



Malicious Activity

Malicious #1: Downloading Copyrighted Materials

Summarize the following:

- Torrent traffic was observed on the network (BitTorrent, TCP and HTTP protocols).
- The user was browsing through animated movies on <http://publicdomaintorrents.info> and downloaded one torrent file - "Betty Boop Rhythm on the Reservation.avi.torrent".
- Packet 69706 is the HTTP GET request for the file, the response including the file is 69719.

The screenshot displays a network traffic analysis tool with three main components:

- Packet List:** A table of network packets with columns for No., Time, Source, Destination, Protocol, Port, and Info.
- Packet Details:** A detailed view of a selected packet (No. 69719) showing its structure and content.
- Video Player:** A small window showing a video frame from "Betty Boop Rhythm on the Reservation.avi".

No.	Time	Source	Destination	Protocol	Port	Info
69706	770.366956400	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_B
69719	770.516249900	files.publicdomaint...	BLANCO-DESKTOP.dogo...	HTTP	59	HTTP/1.1 200 OK (application/x-bittorrent)
69980	771.231145500	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	434	GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%
69995	771.282361800	files.publicdomaint...	BLANCO-DESKTOP.dogo...	HTTP	1084	HTTP/1.1 301 Moved Permanently (text/html)
70122	771.590958400	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	253	GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd
70127	771.609881900	files.publicdomaint...	BLANCO-DESKTOP.dogo...	HTTP	670	HTTP/1.1 301 Moved Permanently (text/html)

Packet Details (No. 69719):

- Internet Protocol Version 4, Src: files.publicdomaintorrents.com (168.215.194.14), Dst: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.0)
- Transmission Control Protocol, Src Port: 80, Dst Port: 49834, Seq: 8621, Ack: 536, Len: 5
- [7 Reassembled TCP Segments (8625 bytes): #69710(1460), #69711(1460), #69712(1460), #69713(1460), #69715(1460), #69717(1320), #69718(1460)]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Sun, 15 Jul 2018 04:17:27 GMT\r\n
 - Server: Apache\r\n
 - Content-Disposition: inline; filename="Betty Boop Rhythm on the Reservation.avi.torrent"\r\n
 - Set-Cookie: PHPSESSID=a42bg863capgr3h\r\n
 - Keep-Alive: timeout=5, max=100\r\n
 - Connection: Keep-Alive\r\n
 - Transfer-Encoding: chunked\r\n
 - Content-Type: application/x-bittorrent\r\n

Video Player: File Name: Betty Boop_Rhythm_on_the_Reservation.avi, File Size: 106.59 MB, Resolution: 720x480, Duration: 00:06:42

Malicious #2: AD Network and Downloaded Malware

Summarize the following:

- Traffic related to a rogue Active Directory server has been observed. Protocols include LDAP, KRB5 (Kerberos), DNS.
- Two users created frank-n-ted.com (10.6.12.12).
- A client that was part of this domain downloaded a malware file called june11.dll. This file appears to be a Trojan.

The screenshot displays a security analysis interface. On the left, a sidebar shows a 'Community Score' of 51/66 and a list of security vendors. The main area is divided into two panes. The top pane shows a table of network traffic with columns: No., Time, Source, Destination, Protocol, Port, and Info. The bottom pane shows a detailed view of a DNS response frame (Frame 55451).

Network Traffic Table:

No.	Time	Source	Destination	Protocol	Port	Info
55451	641.145958800	Frank-n-Ted-DC.frank-n...	DESKTOP-86J4BX.frank-n...	DNS	60440	Standard query response 0x6b8d SRV _ldap._tcp.Default-Fir...
55579	641.712303800	Frank-n-Ted-DC.frank-n...	DESKTOP-86J4BX.frank-n...	DNS	63295	Standard query response 0x31ae SRV _ldap._tcp.Default-Fir...
55607	641.812202100	Frank-n-Ted-DC.frank-n...	DESKTOP-86J4BX.frank-n...	DNS	50100	Standard query response 0x70df SRV _ldap._tcp.Default-Fir...

DNS Response Details (Frame 55451):

- 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface eth0, id 0
- Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel_68:42:d3 (00:11:75:68:42:d3)
- Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
- User Datagram Protocol, Src Port: 53, Dst Port: 60440
- Domain Name System (response)
 - Transaction ID: 0x6b8d
 - Flags: 0x8580 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.frank-n-ted.com: type SRV, class IN, priority 0, weight 100, port 389, target frank-n-te...
 - Answers
 - frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12

Malware Detection Results:

Vendor	Detection
Ad-Aware	Trojan.Mint.Zamg.O
Alibaba	TrojanSpy:Win32/Yakes.8988e849
Antiy-AVL	Trojan.Generic.ASCommon.1BE
Avast	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefenderTheta	Gen:NN.ZedlaF.34062.lu9@aui7OQgi
Cylance	Unsafe
DrWeb	Trojan.Inject3.53106

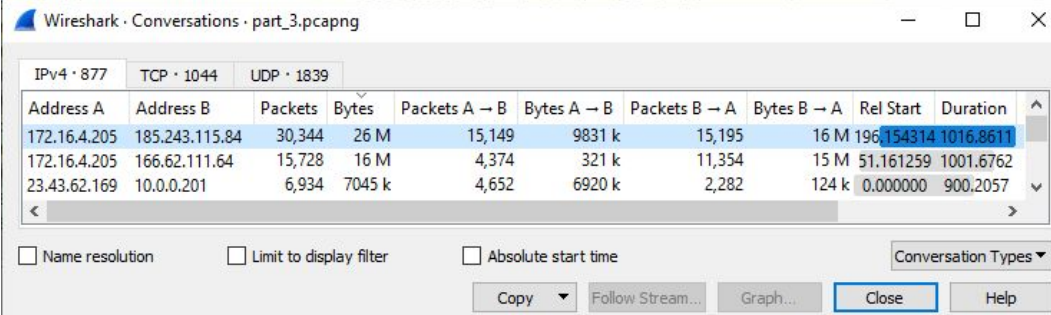
Additional Information:

- CrowdStrike Falcon: Win/malicious_confidence_100% (W)
- Cynet: Malicious (score: 100)
- Elastic: Malicious (high Confidence)

Malicious #3: Infected Windows Machine

Summarize the following:

- What kind of traffic did you observe?
Massive amount of traffic from
185.243.115.84
(b5689023.green.mattingssolutions.co)
- Which protocol(s)?
HTTP (tcp/80)



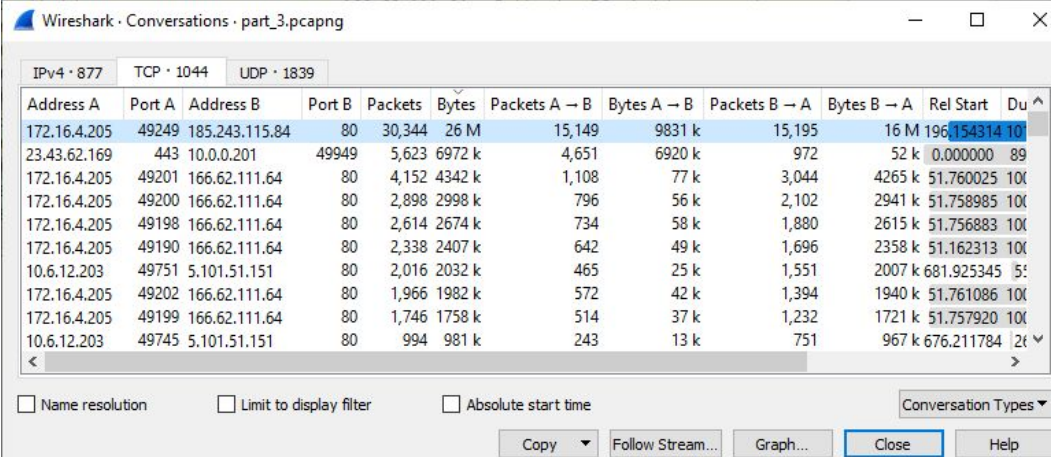
Wireshark · Conversations · part_3.pcapng

IPv4 · 877 TCP · 1044 UDP · 1839

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	1016.8611
172.16.4.205	166.62.111.64	15,728	16 M	4,374	321 k	11,354	15 M	51.161259	1001.6762
23.43.62.169	10.0.0.201	6,934	7045 k	4,652	6920 k	2,282	124 k	0.000000	900.2057

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time Conversation Types ▾

Copy ▾ Follow Stream... Graph... Close Help



Wireshark · Conversations · part_3.pcapng

IPv4 · 877 TCP · 1044 UDP · 1839

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.4.205	49249	185.243.115.84	80	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	1016.8611
23.43.62.169	443	10.0.0.201	49949	5,623	6972 k	4,651	6920 k	972	52 k	0.000000	89
172.16.4.205	49201	166.62.111.64	80	4,152	4342 k	1,108	77 k	3,044	4265 k	51.760025	101
172.16.4.205	49200	166.62.111.64	80	2,898	2998 k	796	56 k	2,102	2941 k	51.758985	101
172.16.4.205	49198	166.62.111.64	80	2,614	2674 k	734	58 k	1,880	2615 k	51.756883	101
172.16.4.205	49190	166.62.111.64	80	2,338	2407 k	642	49 k	1,696	2358 k	51.162313	101
10.6.12.203	49751	5.101.51.151	80	2,016	2032 k	465	25 k	1,551	2007 k	681.925345	51
172.16.4.205	49202	166.62.111.64	80	1,966	1982 k	572	42 k	1,394	1940 k	51.761086	101
172.16.4.205	49199	166.62.111.64	80	1,746	1758 k	514	37 k	1,232	1721 k	51.757920	101
10.6.12.203	49745	5.101.51.151	80	994	981 k	243	13 k	751	967 k	676.211784	21

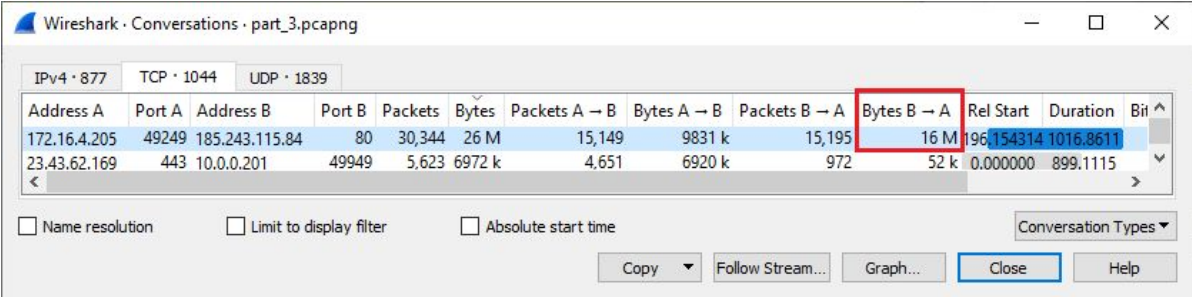
☐ Name resolution ☐ Limit to display filter ☐ Absolute start time Conversation Types ▾

Copy ▾ Follow Stream... Graph... Close Help

Malicious #3 (cont): Infected Windows Machine

Summarize the following:

- What, specifically, was the user doing?
Which site were they browsing?
Downloading from 182.243.115.84



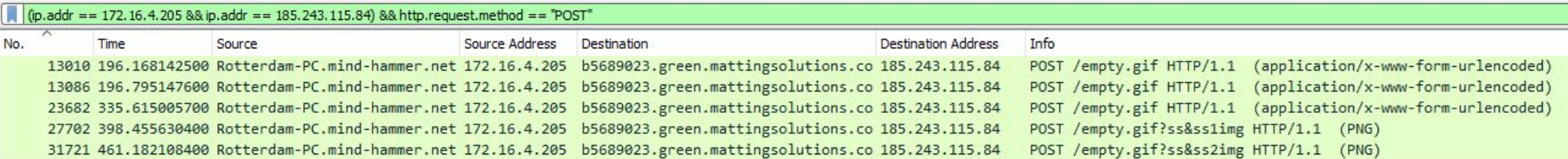
Wireshark · Conversations · part_3.pcapng

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bit
172.16.4.205	49249	182.243.115.84	80	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	1016.8611	
23.43.62.169	443	10.0.0.201	49949	5,623	6972 k	4,651	6920 k	972	52 k	0.000000	899.1115	

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Copy Follow Stream... Graph... Close Help

- Include screenshots of packets justifying your conclusions.



(ip.addr == 172.16.4.205 && ip.addr == 182.243.115.84) && http.request.method == "POST"

No.	Time	Source	Source Address	Destination	Destination Address	Info
13010	196.168142500	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	182.243.115.84	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
13086	196.795147600	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	182.243.115.84	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
23682	335.615005700	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	182.243.115.84	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
27702	398.455630400	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	182.243.115.84	POST /empty.gif?ss&sslimg HTTP/1.1 (PNG)
31721	461.182108400	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	182.243.115.84	POST /empty.gif?ss&sslimg HTTP/1.1 (PNG)

- Include a description of any interesting files.
 - empty.gif would crash the Kali virtual machine when attempting to export it from Wireshark.



The End